RSA Algorithm:-

↓

Ron Rivest, Adi Shamir and Leonard Adleman in 1978.

It is an asymmetric cryptographic algorithm.
(2 keys) i.e public and private key

Public key → Known to all users in N/W.
Private Key → Kept secret, not shareable to all.

If public key of user A is used for encryption, we have to use the private key of some user for decryption.

The RSA scheme is a block cipher (→ Secret, a code) in which the plain text and ciphertext are integers b/w 0 and n-1 for some value n.

---

1. Key Generation: [RSA ALGORITHM]

i) Select 2 large prime numbers 'P' and 'q'.
ii) Calculate $n = P * q$.
iii) Calculate $\phi(n) = (p-1) * (q-1)$ // Euler's toitient function.
iv) choose value of e

$$1 < e < \phi(n) \text{ and } \gcd(\phi(n), e) = 1$$

v) calculate

$$d = e^{-1} \bmod \phi(n)$$

$$ed = 1 \bmod \phi(n)$$

vi) Public key = {e, n}

vii) Private key = {d, n}

2. Encryption.

$C = M^e \bmod n$.

plaintext = $M < n$.
C → ciphertext.

3. Decryption

$M = C^d \bmod n$

Problems:-

1: Using RSA algorithm find public key and Private key w.r.to $p = 3$, $q = 11$ and $M = 31$

Soln: Let $p = 3$, $q = 11$

$n = p * q = 3 * 11 = 33$

$\phi(n) = (p-1) * (q-1) = 2 * 10 = 20$.

so, let $e = 7$ as $1 < 7 < 20$ &
$\gcd(7, 20) = 1$

Now $d = e^{-1} \bmod \phi(n)$.

$de \equiv 1 \bmod \phi(n)$.

$7 * d \equiv 1 \bmod 20$. (Solve by using Euclidean Algorithm also)

$\therefore d = 3$

Since $e = 7$, $d = 3$

Public Key = $\{e, n\} = \{7, 33\}$

Private key = $\{d, n\} = \{3, 33\}$.

Encryption: $C = M^e \bmod n$ Let $M = 31$.

$C = 31^7 \bmod 33$

$31 \equiv -2 \bmod 33$

$(31)^7 \equiv (-2)^7 \bmod 33$

$(31)^7 \equiv -128 \pmod{33}$

$(31)^7 \equiv -(-4) \bmod 33$

$(31)^7 \equiv 4 \pmod{33}$ $\quad [^{0}A\ ^{1}B\ ^{2}C\ ^{3}D\ ^{4}E - - - - 26]$

$\Rightarrow C = 04 = AE.$

$\Rightarrow M = 31 = \underline{DB}$ (plaintext) $\quad \Rightarrow C = 04 = \underline{AE}$ (ciphertext).

Decryption:

$M = c^d \bmod n.$

$M = 4^3 \bmod 33$

$4^3 \equiv 64 \bmod 33$

$M \equiv 31 \bmod 33.$

$\therefore M = 31 = DB.$

---

2) In RSA algorithm if $p = 7$, $q = 11$ and $e = 13$ then what will be the value of d?

Soln: $p = 7, \quad q = 11$

$n = pq = 7 \times 11 = 77.$

$\phi(n) = (p-1)(q-1) = 6 \times 10 = 60.$

Given $e = 13.$

$\Rightarrow 1 < 13 < 60 \ ; \ \gcd(60, 13) = 1.$

To find d:

$d \equiv e^{-1} \bmod (\phi(n))$

$ed \equiv 1 \bmod (\phi(n))$

$13d \equiv 1 \bmod 60.$

$\Rightarrow 60 \mid 13d - 1 \Rightarrow 13d - 1 = 60K$

$\Rightarrow d = \frac{60K + 1}{13}.$

If $K = 8$, $\underline{d = 37}$.

$\therefore$ public key = $\{e, n\} = \{13, 77\}$

Private key = $\{d, n\} = \{37, 77\}$.

**3) Encode STOP using RSA algorithm with key $(n, e) = (2537, 13)$ and $P=43$, $q=59$.

Public key

Soln:- $P=43$, $q=59$.

$n = Pq = 2537$.

$\phi(n) = (P-1)(q-1) = 42 \times 58 = 2436$.

Given $e=13$, $1 < e < 2436 \Rightarrow 1 < 13 < 2436$.

$\therefore \gcd(2436, 13) = 1$.

$M = \text{STOP} = 1819\,1415$ (0 1 2 3 4 5 = A B C D E F ----)

Let $M_1 = 1819$ $M_2 = 1415$.

Encryption:

$C = M^e \bmod n$

$C_1 = M_1^e \bmod n \Rightarrow C_1 = (1819)^{13} \bmod 2537$.

$(1819)^2 \equiv 3308761$.

$C_1 = 2081$

$C_2 = M_2^e \bmod n \Rightarrow C_2 = (1415)^{13} \bmod 2537$.

$C_2 = 2182$.

$C = C_1 C_2 = 2081\,2182$

$C = UHBYHC$.

---

4) If $p=3$, $q=11$ and private key $d=7$ find the public key using RSA algorithm and hence encrypt the number 19.

Soln: $n = p \times q = 33$, $d = 7$.

$\phi(n) = (p-1)*(q-1) = 2*10 = 20$.

To find e:

$1 < e < \phi(n)$

$\Rightarrow 1 < e < 20$.

$\Rightarrow \gcd[e, 20] = 1$

W.K.T $ed \equiv 1 \pmod{\phi(n)}$

$7e \equiv 1 \pmod{20}$

$\Rightarrow 20 / 7e-1$

$\Rightarrow 7e-1 = 20K$.

$\Rightarrow e = \frac{20K+1}{7}$

$\Rightarrow \underline{e=3}$

Given $M = 19 = BJ$.

Encryption: $C = M^e \bmod n$.

$C = 19^3 \bmod 33$.

$C = -2 \times 19 \bmod 33$ $(\because 19^2 \equiv -2 \pmod{33})$

$C = -38 \bmod 33 \equiv -5 \bmod 33$

$C = 28 \bmod 33$

$\therefore C = 28 = CI$

5) Using RSA Algorithm decrypt 09810461 using d=937 and p=43, q=59.

Soln: $n = p*q = 43*59 = 2537$.

$\phi(n) = 42*58 = 2436$.

$C = \underline{0981}\,\underline{0461}$

$C_1 = 0981 \quad C_2 = 0461$.

∴ Required plain text is

$M = C^d \pmod n$

$M_1 = C_1^{937} \pmod{2537}$

$M_1 = (0981)^{937} \pmod{2537}$

$M_1 = 0704$.

$M_2 = C_2^d \pmod{2537}$

$M_2 = (0461)^{937} \pmod{2537}$

$M_2 = 1115$

$M = \underline{07}\,\underline{04}\,\underline{11}\,\underline{15}$

$M = \underline{HELP}$.

** To find powers in Calculator.

Eg:- $5^7 \bmod 33 = 14$

$5\times5\times5\times5\times5\times5\times5 = 78{,}125 \div 33$

$= 2367.424242 - 2367$

$= 0.424242 \times 33$

$= 13.999$

$= 14$.